IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Re application of	:	
L. Paatero	:	Examiner: V. Herring
Serial No. 10/090,426	:	Supervisory Examiner: G. Barron
Filed: February 28, 2002	:	Group Art Unit: 2132

For: **METHOD AND SYSTEM TO ALLOW PERFORMANCE OF PERMITTED ACTIVITY WITH RESPECT TO A DEVICE**

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is in furtherance of the Notice of Appeal that was filed July 16, 2007 along with a Pre-Appeal Brief Request for Review. This Appeal Brief is also in response to the Notice of Panel Decision From Pre-Appeal Brief Review dated August 16, 2007. The final Office Action was dated April 6, 2007 and the Advisory Action was dated June 2007.

I hereby certify that this paper is being deposited with the U.S. Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Briefs-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Margery B. Hood 10/19/07

Margery B. Hood Date

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Nokia Corporation, a corporation organized under the laws of Finland.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

There are no related appeals or interferences.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-27, 35-43, 45, and 47-50 are pending in the application and stand rejected. Applicant notes that this status of claims is correctly stated in the Advisory Action, but is incorrectly stated in the Notice of Panel Decision From Pre-Appeal Brief Review. The Notice of Panel Decision From Pre-Appeal Brief Review incorrectly stated that claim 46 is pending.

Claim 46 was cancelled in response to the final office action, on 7 June 2007. Also on 7 June 2007, Applicant amended the independent claims to include the limitations of claim 46. The Advisory Action subsequently stated that those amendments of 7 June 2007 were entered for purposes of appeal. Claims 28-34, and 44 were cancelled prior to the final Office Action.

The rejection of claims 1-27, 35-43, 45, and 47-50 is now being appealed.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

Amendments were submitted after the final Office Action, and all amendments have been entered, according to the Advisory Action. As mentioned above, the Notice of Panel Decision From Pre-Appeal Brief Review incorrectly stated that claim 46 is pending, when actually its limitations were inserted into the independent claims after the final Office Action (i.e. claim 46 was cancelled).

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The independent claims are 1, 20, 26, 41, and 49.

Independent claim 1 recites a method for embedding a role certificate in a device (see page 3, lines 1-9; page 3, line 24 thru page 4, line 2; page 6, line 29 thru page 7, line 7 of the application as originally filed). The role certificate identifies at least one permitted activity that at least one party is allowed to perform with respect to the device (see page 7, line 30 thru page 8, line 13; page 9, lines 3-8; page 9, line 27 thru page 10, line 2; page 10, lines 10-19). The role certificate is generated by a certification authority (see page 3, line 25 thru page 4, line 2; page 6, lines 1-20, page 7, lines 23-29; page 7, line 30 thru page 8, line 13). This can be seen at FIG. 2, step 30.

Also according to claim 1, information regarding a public key is embedded in that device, and the public key corresponds to the private key used by the certification authority to sign the role certificate (paragraphs 13; page 6, lines 1-20; page 6, line 29 thru page 7, line 7; page 7, lines 8-14; page 7, line 30 thru page 8, line 13), as shown in step 32 of FIG. 2. As shown in step 34 of FIG. 2, the device is run so as to verify the role certificate, using the aforementioned information regarding the certification authority public key so that said at least one permitted activity can be activated within the device the party if the role certificate is verified (see page 7, lines 15-22; page 9, lines 3-8). Furthermore, the party communicates with the device to perform the permitted activity, only after the role certificate is embedded in the device (see page 3, line 25 thru page 4, line 2; page 7, lines 15-22; page 9, lines 9-15), as seen in step 44 of FIG. 2. The party performs the permitted activity by establishing a wireless connection to the device, and the role certificate also identifies the party (see page 3, lines 10-21).

The limitations of the other independent claims 20, 26, 41, and 49 are similar to the limitations of claim 1. In the role certificate mechanism of independent claim 20, there is a memory 16 as seen in FIG. 1, and there is also a processor 14; independent means plus function claim 49 corresponds to role certificate claim 20. Independent method claim 41 is similar to independent method claim 1, and several features of

independent claim 41 are also described in the application as originally filed, at page 5, lines 7-12; page 7, lines 9-11; and page 3, line 5. Claim 26 is also a means plus function claim for performing the steps of claim 1, and thus the relevant portions of the specification include those already cited with regard to claim 1, above, with the structure shown in FIG. 1.

All of the independent claims (1, 20, 26, 41, and 49) also say that at least one party performs at least one permitted activity by establishing a wireless connection to the device, and the role certificate identifies that party. These important features are discussed, for example, at page 3, line 25 thru page 4, line 2; page 7, lines 15-22; page 9, lines 9-15 of the specification as originally filed.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

All of the independent claims (i.e. claims 1, 20, 26, 41, and 49), were rejected at page 3 of the final Office Action as being anticipated under 35 U.S.C. § 102(e) by *Doyle et al* (U.S. Pat. No. 6,968,453). Dependent claim 46 was also rejected on the same grounds.

The independent claims were amended after the final Office Action to include the limitations of claim 46. Those after-final amendments were entered, according to the Advisory Action. Applicant is not presenting any of the other dependent claims for review.

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The Advisory Action stated the following: "applicant has repeated the argument that Hind is not validly incorporated by reference in the disclosure of Doyle et al. However, this does not address the rejections of the independent claims...." However, the Advisory Action entered an amendment of the independent claims which incorporated the limitations of claim 46 into the independent claims, and the final Office

Action *did* utilize incorporation by reference to reject claim 46. Consequently, the statement just quoted from the Advisory Action is incorrect.

Claim 46 was rejected at page 16 of the final Office Action (last full paragraph), in reliance upon column 11, line 18 of *Doyle* where "referenced inventions" are cited. Those "referenced inventions" are described at column 8, lines 5-15 of *Doyle* as including *Hind* (U.S. Patent Application 09/614,983 subsequently issued as U.S. Patent No. 6,976,163). Thus, if *Hind* is not validly incorporated by reference in the disclosure of *Doyle*, then the rejection of claim 46 in the final Office Action was improper, and therefore all of the present independent claims (which now contain the limitations of claim 46) should be allowed.

Applicant respectfully submits that the *Doyle* reference does not validly incorporate *Hind* for purposes of anticipating the limitations of the present independent claims. The purported incorporation by reference of *Hind* into *Doyle* occurs at column 8, lines 5-15 of *Doyle*, but *Doyle* never directs attention to any specific portions of *Hind*, much less the specific portions of *Hind* that are relied upon at page 16 of the final Office Action to reject Applicant's claim 46 (which has now been inserted into the present independent claims). The Federal Circuit explained in *Advanced Display v. Kent State*, 54 USPQ2d 1673, 1679 (Fed. Cir. 2000) (emphasis added):

> Material not explicitly contained in the single, prior art document may still be considered for purposes of anticipation if that material is incorporated by reference into the document....To incorporate material by reference, the host document must identify with ***detailed particularity what specific material*** it incorporates and clearly indicate where that material is found in the various documents. (emphasis added)

Doyle simply did not do that with regard to the purportedly incorporated *Hind* reference. *Doyle* did not indicate with detailed particularity — or any particularity at all — what specific material it was incorporating from *Hind*, or where that material can be found in *Hind*.

The final Office Action stated at page two that the Examiner is no longer relying upon *Hind* (U.S. Patent No. 6,976,163). However, the final Office Action repeatedly

relies upon column 11, line 18 of *Doyle*, which purports to incorporate "the referenced inventions" such as *Hind*. See especially page 16 of the final Office Action, at the end of the last full paragraph ("note column 11, line 18"). The only ground in the final Office Action for rejecting claim 46 (which has been inserted into the present independent claims after final) is the *Hind* reference.

Applicant therefore respectfully submits that a 102(e) rejection is inappropriate here. The *Doyle* reference does not validly incorporate the *Hind* reference, for purposes of this anticipation rejection under 35 U.S.C. § 102(e), for the reasons explained in *Advanced Display v. Kent State* (quoted above).

The Advisory Action states that Applicant's argument about the validity of the incorporation by reference "does not address the rejections of the independent claims." However, that is incorrect, because the limitations of claim 46 have been inserted into independent claim 1 after final, and the Advisory Action entered that amendment.

Applicant respectfully emphasizes that neither the final Office Action nor the Advisory Action cited ***any*** portion of *Doyle* whatsoever to reject the limitations of claim 46 (now in claim 1), other than *Doyle's* invalid incorporation of *Hind* at column 11, line 18. Without *Hind*, *Doyle* does not teach or suggest the limitations of claim 46 (now in claim 1), nor has the Office pointed to anything in *Doyle* that does so.

Because the cited *Doyle* reference does not teach or suggest critical elements of the present independent claims, it is respectfully submitted that those claims are novel and patentable. Thus, allowance of the pending claims is respectfully requested.

For these reasons, Applicant respectfully submits that the rejections of the final Office Action have been shown to be inapplicable, and respectfully requests that the Board reverses the rejections to the pending independent claims 1, 20, 26, 41, and 49. If any additional fee is required for submission of this Appeal Brief, the Commissioner is hereby authorized to charge Deposit Account No. 23-0442.

Respectfully submitted,

Date: 19 Oct 2007

Andrew T. Hyman
Attorney for the Appellant
Registration No. 45,858

ATH/mbh
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955

CLAIMS APPENDIX

The claims involved in the appeal are as follows:

1. (Previously Presented) A method, comprising:

embedding a role certificate in a device, wherein the role certificate identifies at least one permitted activity that at least one party is allowed to perform with respect to the device, and wherein the role certificate is generated by a certification authority;

embedding at least information regarding a public key in said device, the public key corresponding to the private key used by the certification authority to sign the role certificate; and

running the device so as to verify the role certificate using said information regarding the certification authority public key so that said at least one permitted activity can be activated within the device by said at least one party if the role certificate is verified,

wherein the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device,

wherein the at least one party performs the at least one permitted activity by establishing a wireless connection to the device, and

wherein the role certificate also identifies the at least one party.

2. (Original) A method as defined in claim 1, wherein the role certificate includes information regarding a control security level for said device so that the device only allows said at least one permitted activity to be a type of action which is within the security level of the device as defined by the role certificate.

3. (Original) A method as defined in claim 2, wherein the security level defined by the role certificate allows a type of software code to be downloaded, and/or installed, and/or run on said device by said at least one party.

4. (Original) A method as defined in claim 3, wherein the type of software code is from the group of types of software code consisting of test code, production code and special code.

5. (Original) A method as defined in claim 4, wherein the special code can be code linked to a specific at least one party.

6. (Original) A method as defined in claim 3, wherein the role certificate further contains information with regard to a specific party of said at least one party that can download, and/or install, and/or run said type of software code.

7. (Original) A method as defined in claim 1, wherein the role certificate further contains information with regard to a specific party of said at least one party that can activate the at least one permitted activity within the device.

8. (Original) A method as defined in claim 7, wherein said information with regard to a specific party is a hash of information identifying said specific party's public key, and wherein the device validates said specific party by receiving said information identifying said specific party's public key, and hashing this information and comparing the hash value to the hash value contained in the role certificate so that if the hash values are equal, then the specific party is permitted to activate the at least one permitted activity.

9. (Original) A method as defined in claim 7, wherein said specific party is a group of entities.

10. (Original) A method as defined in claim 1, wherein the embedding of the role certificate into the device is performed after the information regarding the public key of the CA is embedded into the device.

11. (Previously Presented) A method as defined in claim 1, wherein the information

regarding the certification authority public key is embedded in the device in a tamper resistant area.

12. (Original) A method as defined in claim 11, wherein the tamper resistant area of the device is a portion memory in the device such that any modification of information stored therein can be ascertained.

13. (Original) A method as defined in claim 1, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party.

14. (Previously Presented) A method as defined in claim 1, wherein the certification authority is a root certification authority.

15. (Original) A method as defined in claim 1, wherein the device is a wireless device.

16. (Previously Presented) A method as defined in claim 1, wherein the certification authority is any entity other than said at least one party.

17. (Original) A method as defined in claim 1, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity.

18. (Original) A method as defined in claim 17, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity.

19. (Previously Presented) A method as deemed in claim 1, wherein said information regarding the certification authority public key is a hash value of said certification authority public key.

20. (Previously Presented) A role certificate mechanism, comprising:

memory containing a role certificate, wherein the role certificate is configured to identify at least one activity permitted to be activated within a device in response to a communication from at least one party, and further wherein the memory contains information regarding a first key corresponding to a second key used to sign the role certificate; and

processor configured to run the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device,

wherein the role certificate mechanism is configured to receive the communication only after the role certificate is embedded in said mechanism,

wherein the role certificate is configured to allow the at least one party to perform the at least one permitted activity by establishing a wireless connection to the device, and

wherein the role certificate also identifies the at least one party.

21. (Original) A role certificate mechanism as defined in claim 20, wherein the memory has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area.

22. (Original) A role certificate mechanism as defined in claim 20, wherein the role certificate further includes information regarding the identity of a third party, and wherein the means for verifying the role certificate includes means for reading said third party identity; wherein the role certificate mechanism further comprises means for receiving information from a third party and comparing at least a portion of said received information with the read third party identity from said role certificate, and if the comparison is the same, allowing said third party to perform said at least one activity on said device.

23. (Original) A role certificate mechanism as defined in claim 22, wherein said device is a mobile phone.

24. (Original) A role certificate mechanism as defined in claim 20, wherein said device is a mobile phone.

25. (Original) A role certificate mechanism as defined in claim 20, wherein said information regarding the first key is a hash of said first key.

26. (Previously Presented) An apparatus or system, comprising:

means for embedding a role certificate in a device, wherein the role certificate identifies at least one permitted activity that is allowed to be performed by at least one party with respect to the device, and wherein the role certificate is generated by a certification authority;

means for embedding information regarding a public key in said device, the public key corresponding to the private key used by the certification authority to sign the role certificate; and

means for running the device so as to verify the role certificate using said information regarding the certification authority public key so that said at least one permitted activity can be activated within the device by said at least one party,

wherein the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device

wherein the role certificate is configured to allow the at least one party to perform the at least one permitted activity via a wireless connection to the device, and

wherein the role certificate also identifies the at least one party.

27. (Original) An apparatus as defined in claim 26, wherein the role certificate includes information regarding a control security level for said device so that the means for running the device provides that the at least one permitted activity to only be a type of action which is within the security level of the device as defined by the role certificate.

28. CANCEL

29. CANCEL.

30. CANCEL.

31. CANCEL.

32. CANCEL.

33. CANCEL.

34. CANCEL.

35. (Previously Presented) An apparatus as defined in claim 26, wherein the information regarding the certification authority public key is embedded in the device in a tamper resistant area.

36. (Previously Presented) An apparatus as defined in claim 26, wherein said information regarding the certification authority public key is a hash of said certification authority public key.

37. (Original) An apparatus as defined in claim 26, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party.

38. (Original) An apparatus as defined in claim 26, wherein the device is a wireless device.

39. (Original) An apparatus as defined in claim 26, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity.

40. (Original) An apparatus as defined in claim 39, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity.

41. (Previously Presented) A method, comprising:

embedding a role certificate applicable to a plurality of devices in an individual device, wherein the role certificate specifies at least one permitted activity that is allowed to be performed by at least one party as applied to the plurality of devices, and wherein the role certificate is generated by a certification authority;

embedding at least information regarding a public key applicable to the plurality of devices in said individual device, the public key corresponding to the private key used by the certification authority to sign the role certificate; and

running the individual device so as to verify the role certificate using said information regarding the certification authority public key so that said at least one permitted activity can be activated within the individual device by said at least one party if the role certificate is verified,

wherein the at least one party communicates to perform the permitted activity, only after the role certificate is embedded in said individual device,

wherein the at least one party performs the at least one permitted activity by establishing a wireless connection to the device, and

wherein the role certificate also identifies the at least one party.

42. (Previously Presented) The method of claim 41, wherein said individual device is also embedded with at least one different role certificate.

43. (Previously Presented) The method of claim 42, wherein one of the at least one different role certificate specifies at least a third party or a group or a device, and wherein the at least one permitted activity is not conducted if the one of the at least one different role certificate does not match said at least a third party or a group or a device.

44. CANCEL

45. (Previously Presented) The method of claim 1, wherein the role certificate includes a name of the certification authority that issued the certificate, a serial number, and an expiration date.

46. CANCEL

47. (Previously Presented) The method of claim 1, wherein the role certificate is embedded in said device during manufacture.

48. (Previously Presented) The mechanism of claim 20, wherein the role certificate is embedded in said mechanism during manufacture.

49. (Previously Presented) Apparatus, comprising:

means for storing a role certificate, wherein the role certificate is configured to identify at least one activity permitted to be activated within a device in response to a communication from at least one party, and further wherein the means for storing the role certificate contains information regarding a first key corresponding to a second key used to sign the role certificate; and

means for running the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device,

wherein the communication occurs only after the role certificate is embedded in said mechanism,

wherein the role certificate is configured to allow the at least one party to perform the at least one permitted activity via a wireless connection to the device, and

wherein the role certificate also identifies the at least one party.

50. (Previously Presented) An apparatus as defined in claim 49, wherein the means for storing the role certificate has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.